Exhibit A

AFFIDAVIT IN SUPPORT OF A SEIZURE WARRANT

I, Troy M. Capser, Special Agent with Homeland Security Investigations, being duly sworn, deposes and states under penalty of perjury that the following is true to the best of my information, knowledge, and belief.

AFFIANT BACKGROUND AND KNOWLEDGE

1. I am a Special Agent with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI) and have been since 2001. In my experience in federal law enforcement, I have participated in and conducted numerous complex criminal investigations including investigations of India-based call centers engaged in various telephone and email extortion schemes. I received extensive instruction and training at the Federal Law Enforcement Training Center (FLETC) relating to general investigative techniques, electronic surveillance, rules of evidence and legal principles and statutes pertaining to criminal violations of federal law, including but not limited to, U.S. customs and immigration offenses, money laundering, currency violations, wire fraud, mail fraud, conspiracy and document and benefit fraud.
2. By virtue of my employment as a Special Agent, the federal crimes I am assigned to investigate include, but are not limited to, violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1001 (false statements), 18 U.S.C. § 1028 (identity theft), 18 U.S.C. § 1028A (aggravated identity theft), 18 U.S.C.§ 1343 (wire

fraud), 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 1344 (bank fraud), and 18 U.S.C. § 1956 (money laundering). As a Special Agent I am personally familiar with and have used all normal methods of investigation, including, but not limited to, visual surveillance, electronic surveillance, informant and witness interviews, interrogation, and undercover operations. I have performed various tasks, which include, but are not limited to: functioning as a surveillance agent; participating in the tracing of monies and assets obtained by illicit activities within the United States and abroad; interviewing witnesses, cooperating individuals and informants; functioning as a case agent; authoring and executing Federal search warrants for evidence of crimes against the United States; and participation in the arrests of numerous individuals for violations of the United States Code.

3. I have participated in the execution of search and seizure warrants involving electronic evidence and have been extensively involved in investigations of wire fraud and money laundering crimes related to criminal India-based call centers. I have had many discussions with other experienced law enforcement officers and have conducted, and been present at, interviews of convicted money launderers and cooperating defendants concerning how proceeds of telephone scams are moved. I know that payment processors and runners often hold proceeds traceable to their criminal call center activities in the form of United States currency, funds in bank accounts, high-value personal property items, and real property.

4. Because I am submitting this affidavit for the limited purpose of establishing probable cause for the requested seizure warrants, I have not included in this affidavit every detail I know about this investigation. Rather, I have included only the information necessary to establish probable cause for the requested seizure warrants.

5. The facts set forth in this affidavit are based on my personal knowledge, including what I have learned through my training and experience as a law enforcement officer, my review of documents and other records obtained in the course of this investigation, and information I have obtained in the course of this investigation from witnesses having personal knowledge of the events and circumstances described herein and other law enforcement officers.

APPLICABLE CRIMINAL LAW

6. Title 18 U.S.C. § 1343 provides:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

7. Title 18 U.S.C. § 1349 provides:

> Any person who *attempts or conspires* to commit any offense under this chapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

PROPERTY TO BE SEIZED

8. This Affidavit is submitted in support of the Application made by the United States of America for a Seizure Warrant authorizing the seizure of up to **$146,100** in funds on deposit in **JP Morgan Chase Bank**[1] Account 00000851063971 titled to 5745 LITTLE NECK LLC, 5745 256TH ST, LITTLE NECK NY 11362-2140 hereinafter referred to as "**TARGET ACCOUNT**."

9. For the reasons set forth below, I submit that up to $146,100 in funds on deposit in the **TARGET ACCOUNT** are:

   a. Funds traceable to, and are therefore proceeds of, a wire fraud offense or offenses committed in violation of Title 18 U.S.C. § 1343;

   b. Subject to civil forfeiture under Title 18 U.S.C. §§ 981(a)(1)(C);

   c. Subject to criminal forfeiture under Title 18 USC § 981(a)(1)(c) & Title 28 USC § 2461;

   d. Subject to seizure via civil seizure warrant under Title 18 U.S.C. § 981(b)(2); and

   e. Subject to seizure via a criminal seizure warrant under Title 21 USC § 853(e) & (f) by 18 USC § 982(b)(1).

BACKGROUND ON SCHEME TO DEFRAUD

10. Beginning in late 2013, India-based call centers began industrial-scale U.S. Government impersonation scams which convinced many victims that they were subject to arrest/deportation if they did not immediately follow the instructions of

[1] Chase Bank has branches throughout the United States and is headquartered in New York, New York, which is in the Southern District of New York.

persons purporting to represent the U.S. Government. These instructions included instructions on how to pay money owed to the U.S. Government. Over the years these scams evolved and included impersonation of additional agencies including the Social Security Administration as well as the Federal Trade Commission. These India-based call center scams have recently shifted much of their volume to Microsoft Pop Up and Amazon email refund scams impersonating Microsoft, Amazon, and the victim's bank. These Microsoft and Amazon tech support refund scams still include U.S. Government impersonation when necessary to convince victims.

11. These scams, directed from India-based call centers, convince victims to pay fictitious fines/penalties using a variety of methodologies including cash via FedEx/UPS, purchase of prepaid debit / general purpose reloadable cards (GPR) cards, direct bank wire transfer, Western Union / MoneyGram wires, purchase of iTunes gift cards, as well as many others. Victims sending FedEx/UPS shipments of cash are instructed by callers to overnight ship U.S. currency to various fake names purporting to be government officials or attorneys who were receiving the funds on behalf of the U.S. Government. These fake names corresponded to names used on false identity documents held by runners to receive the victims' shipments at FedEx/UPS pickup locations. Victim funds moved through iTunes and prepaid debit card products are commonly converted to bitcoin cryptocurrency wallets.

12. India-based call centers and their networks of payment processors[2] (including organized Chinese money laundering teams) have adapted a new process built on tech support scams in which they impersonate Microsoft and claim to be protecting the victim from "Hackers" who have compromised the victim's computer and bank account(s). This scam also includes informing victims that their identities have been used by "Hackers" to purchase child pornography. In order to clear the charges victims are often told that Microsoft needs to scan their computers for long periods of time in order to track down the "Hackers." This process also includes daily long-duration calls with the scammers as well as the scammers having complete control over victim computers using remote access tool software downloaded to victim computers.

13. The scammers often attempt to physically and mentally exhaust victims over long periods of time before convincing victims their life savings needs to be moved in order to protect their accounts from "Hackers." When victims resist the scammers often impersonate law enforcement. Scammers impersonating Fraud Departments of various U.S. banking institutions sometimes explain to victims that the Hackers have already sent a wire from their account and the only way to block it is to send a second wire which places a fraud block on the account.

[2] Criminal India-based call centers often refer to victims as "customers" and movement of their funds as "payment processing." The "payment processor" designation refers to conspirators located in India and/or the United States who act as an intermediary between the call centers and the runners in order to receive victim funds and distribute them in coordination with other payment processors and hawaladars acting in concert with the greater conspiracy.

14. Organized crews of Runners laundering cash proceeds of U.S. Government and tech support imposter telephone scams often keep a portion of the funds and transfer the rest using cash withdrawals and/or outgoing wires.

PROBABLE CAUSE FOR ISSUANCE OF SEIZURE WARRANT

15. In June 2022, Homeland Security Investigations (HSI) Fayetteville, Arkansas, received a police report detailing that an individual residing in Bella Vista, Arkansas, which is in the Western District of Arkansas, Fayetteville Division, lost his life's savings of more than $300,000 as a result of a phone-based scam involving representations of an individual fraudulently claiming to be a Microsoft representative. The phone number involved, which has since been linked to numerous other scams, was traced to an India-based IP address. Consequently, HSI Fayetteville field office began reviewing and investigating related fraud referrals involving victims of the Microsoft Pop Up and other related scams in the Western District of Arkansas, which are likewise happening across the United States. HSI Fayetteville field office has identified more than $700,000 in local victim losses since February of 2022, and more than $10,000,000 in nationwide losses related to this scheme, which appears to originate from India.

16. On August 17, 2022, your affiant spoke with a Kalispell resident in the District of Montana, referenced hereafter as N.P., who stated that on or around July 22, 2022, she had received an email purporting to be from Microsoft support [this email is believed to have been deleted by the India-based scammers after gaining remote

access to victim's computer]. The victim called the number in the email and believed she was speaking with Microsoft technical support. The Microsoft imposter using the name "Sam" gained remote access to the victim's computer through remote access tools including AnyDesk and then directed victim to login to their bank account to receive a refund from Microsoft. The scammers then directed victim to a fake "refund form" in which the victim filled out $6,000. After typing $6,000 an extra zero was added by the scammers who also had control over victim's computer. The refund form reflected a refund to the victim of $60,000 and the scammers convinced her that too much money had been refunded. The scammers appear to have edited the html code on the victim's online banking login in order to falsely reflect to the victim that she had received the refund in the amount of $60,000. The victim was convinced that she had made the clerical error to receive too large of a refund and she needed to wire $60,000 back to the purported "Microsoft" representative. The fake Microsoft representative also connected victim with another co-conspirator using the name "Jacob" who purported to be from the Park Side Credit Union fraud department where the victim banks. The victim was further told by the scammers that her identity had been used to make purchases on porn websites in China and that dummy transactions were needed to track the hackers and/or reverse the wires they had

already sent. Your affiant is familiar with this scheme that is known as a classic technical support refund scam.[3]

17. On or around 8/16/2022, victim N.P. (Kalispell, MT), at the instruction of scammers purporting to represent her bank, wired $60,000 to the following recipient:

> Bank: JP Morgan Chase Bank (4 New York Plaza, Floor 15, New York, NY 10004)
> Recipient: SUPER KITTY TRADING CO
> Recipient Address: 1234 Santa Anita Avenue, South El Monte, CA 91733
> Recipient Account # 20000012584298
> Routing # 021000021

18. On August 17, 2022, SA Dylan Critten (HSI Fayetteville, Arkansas) spoke with C.B., A.S., and J.S. (Dallas, Texas) who are the wife/son/daughter of victim P.J. SA Critten also spoke with P.J. C.B. and J.S. related to SA Critten that P.J. is 70 years old and cognitively impaired. P.J. had been on his phone and computer for long periods of time, and they did not understand what was going on. P.J. had been stating that he needed to contact Norton because of a mistake he made. P.J.

[3] Tech support refund scams occur when a scammer obtains remote access to a victim's computer, instructs victim to login to their online banking account, and then brings up some version of a refund form. The victim is instructed that they are receiving a refund for services not provided. The victim is instructed to type in the amount of the refund on the non-reversable form. As they finish typing the scammer adds zeroes to the number to make it appear to the victim that the victim was refunded a large amount of money. The scammers convince the victim that they are at fault for the error. The scammer instructs the victim that they will lose their job for refunding too much money to the victim. As they are building this story up the scammer quickly edits the html code on the victim's online banking account webpage which falsely makes it appear to the victim that they received a large refund into their bank account. The victim is convinced that they received too much money back in error and is instructed by the scammers to wire funds to various third-party accounts which are received by networks of U.S.-based money laundering runners.

and family provided SA Critten the original email that came from "Norton" which had a phone number that P.J. called. The email originated from a Gmail account. The phone number originated from a Ring Central Inc. VoIP customer. SA Critten served Google with a Preservation Request for the email account in order to preserve evidence for legal process. P.J. further confirmed he had been a victim of a Norton tech support refund scam and provided wire information to SA Critten. On 8/16/2022, P.J. sent the following $24,600 wire to the same recipient with same address (separate account number) as N.P. in Kalispell, MT:

Bank: JP Morgan Chase (875 Saw Mill River Rd., New York, NY 10502)
Recipient: SUPER KITTY TRADING CO
Recipient Address: 1234 Santa Anita Avenue, South El Monte, CA 91733
Recipient Account # 20000012593848
Routing # 021000021

On 8/17/2022, P.J. sent the following wire for $21,500 which was funded with a home equity loan

Bank: JP Morgan Chase Bank (4 New York Plaza, Floor 15, New York, NY 10004)
Recipient: FOLSOM YAN TRADING CO
Recipient Address: 14840 E PROCTOR AVE, LA PUENTE, CA 91746
Recipient Account # 20000013016846
Routing # 021000021

19. On August 18, 2022, SA Critten spoke with J.F. (Quakertown, PA), aged 85, who was also a victim of a Best Buy Geek Squad tech support refund scam. J.F. was convinced by Best Buy Geek Squad imposters that he had been refunded too much money in error and on 08/16/2022 sent a $40,000 wire (using a home equity line of credit) to the same recipient (separate account number) as N.P. and P.J.

Bank: JP Morgan Chase Bank (4 New York Plaza, Floor 15, New York, NY 10004)
Recipient: SUPER KITTY TRADING CO
Recipient Address: 1234 Santa Anita Avenue, South El Monte, CA 91733
Recipient Account # 20000013067310
Routing # 021000021

On August 17, 2022, J.F., at the direction of the scammers, had attempted another $53,000 wire (also using a home equity line of credit) to FOLSOM YAN TRADING CO (14840 E PROCTOR AVE, LA PUENTE, CA 91746), which the local bank held up and referred to the fraud department.

20. Each of the SUPER KITTY TRADING CO accounts 20000012584298, 20000012593848, and 20000013067310 (which N.P., P.J., and J.F. wired funds to) as well as one additional account 20000013016843 (which is also believed to have received victim funds) are contained within SUPER KITTY TRADING COMPANY's Alipay account. The Alipay account titled to SUPER KITTY TRADING COMPANY has shown no transactions prior to 08/16/2022. On 08/16/2022, Alipay user SUPER KITTY TRADING COMPANY remitted funds of $154,500 to newly opened TARGET ACCOUNT. Funds were remitted as two separate wires, at 16:02:31 and 16:28:22.

21. JPMC and your affiant believe that the funds sent from Alipay user SUPER KITTY TRADING COMPANY to 5745 LITTLE NECK LLC were the funds remitted to SUPER KITTY TRADING COMPANY, which victims N.P. (Kalispell, MT), P.J. (Dallas, TX), and J.F. (Quakertown, PA) wired funds to. Additionally, Alipay appears to be allowing hundreds of other dummy accounts,

also having multiple sub-accounts, which end with "TRADING CO." These accounts all appear to have been opened in the last few months for the sole purpose of money laundering. JPMC has identified eight victims who sent, or attempted to send, wires to SUPER KITTY TRADING COMPANY on 08/16/2022 and 08/17/2022.

22. Additionally, SA Critten in conjunction with your affiant, conducted records searches on the principals of KITTY TRADING CO and FOLSOM YAN TRADING and found no legitimate individuals that can be verified.

23. As a result of these materially false and fraudulent pretenses, representations, and promises, these victims wired funds from the District of Montana and elsewhere to the conspirators. It was further part of the conspiracy that KITTY TRADING CO and other conspirators received wire transfers into the **TARGET ACCOUNT** from victims, and forwarded funds onward to other conspirators, thus concealing the control of the proceeds of this specified unlawful activity.

APPLICABLE ASSET FORFEITURE PROVISIONS

24. Title 18 U.S.C. § 981(a)(1)(C) allows for civil forfeiture of any real or personal property which is proceeds or derived from proceeds that are traceable to a violation of Title 18 U.S.C. § 1343, Wire Fraud.

25. Title 18 USC § 981(a)(1)(c) & Title 28 USC § 2461 allow for the criminal forfeiture of any real or personal property which is proceeds or derived from proceeds that are traceable to a violation of Title 18 U.S.C. § 1343, Wire Fraud.

26. Title 18 U.S.C. Title 18 U.S.C. § 984 provides:

> (a)(1) In any forfeiture action in rem in which the subject property is cash, monetary instruments in bearer form, funds deposited in an account in a financial institution (as defined in section 20 of this title), or precious metals—
>
> (A) it shall not be necessary for the Government to identify the specific property involved in the offense that is the basis for the forfeiture; and
>
> (B) it shall not be a defense that the property involved in such an offense has been removed and replaced by identical property.
>
> (2) Except as provided in subsection (b), *any identical property found in the same place or account as the property involved in the offense that is the basis for the forfeiture shall be subject to forfeiture under this section.*
>
> (b) No action pursuant to this section to forfeit property not traceable directly to the offense that is the basis for the forfeiture may be commenced more than 1 year from the date of the offense.

(emphasis added).

27. Thus, if an account received funds subject to forfeiture, it is not necessary that the Government directly trace the funds in the account to the offense that is the basis for forfeiture in order to seize and forfeit funds up to the amount identified as proceeds from the offense. Here, that means that up to $146,100 in proceeds from N.P., P.J., and J.F. that are available in the **TARGET ACCOUNT** are subject to forfeiture even though not directly traced to the offense giving rise to forfeiture.

28. In this case, interstate wires in connection with the above-described tech support refund scheme, have been deposited into the **TARGET ACCOUNT**.

29. Your affiant has identified the funds in the **TARGET ACCOUNT** as the proceeds of wire fraud, and it is the intention of the United States to remit and return the seized funds of $60,000 to N.P. (Kalispell, MT), $40,000 to J.F. (Quakertown, PA), and $46,100 to P.J. (Dallas, TX) should this seizure warrant be granted.

CONCLUSION

30. Based on the foregoing, I submit there is probable cause to believe that funds up to $146,100 on deposit in Chase Bank in the **TARGET ACCOUNT** are:

a. Funds traceable to, and are therefore proceeds of, a wire fraud offense or offenses committed in violation of Title 18 U.S.C. § 1343;

b. Subject to civil forfeiture under Title 18 U.S.C. §§ 981(a)(1)(C);

c. Subject to criminal forfeiture under Title 18 USC § 981(a)(1)(c) & Title 28 USC § 2461;

d. Subject to seizure via civil seizure warrant under Title 18 U.S.C. § 981(b)(2); and

e. Subject to seizure via a criminal seizure warrant under Title 21 USC § 853(e) & (f) by 18 USC § 982(b)(1).

/s/ Troy M. Capser
Troy M. Capser
Special Agent
Homeland Security Investigations

Sworn to before me over the telephone and signed by me pursuant to Fed. R. Crim P. 4.1 and 4(d) this 23rd day of August, 2022.

Kathleen L. DeSoto
Honorable Kathleen L. DeSoto
United States Magistrate Judge
District of Montana